Cyber security of connected vehicles

Best practices

BV - CAR CYBER SEC - 001 / 20161003

Move Forward with Confidence

BUREAU VERITAS

Published by BUREAU VERITAS SA.
Co-written by BUREAU VERITAS SA and DEVOTEAM.

devoteam

BUREAU VERITAS
1828

CONTENTS

FIRST STEPS

OBJECTIVES

ANNEXES

FIRST STEPS

1. INTRODUCTION 6
1.1. Purpose 6
1.2. State of the art 6
1.3. Automotive ecosystem 7
1.4. Methodology 7
1.5. Guidelines structure 8
1.6. Definitions 9
1.7. Abbreviations 10

1. Introduction

1.1. Purpose

These guidelines are written to address an emerging issue for automotive manufacturers and suppliers: how to secure their vehicles against cyber threats?

1.2. State of the art

For several years now, vehicles have been embedding features exposed to cyber attacks. Those attacks can affect Confidentiality, Availability and/or Integrity properties of the vehicle, for example:

- ability to intercept exchanged data in the vehicle,
- ability to immobilize a vehicle fleet,
- ability to control and modify the vehicle remotely or to steal it.

Vulnerabilities in current vehicles exist and they are even more present in the connected vehicles. The challenges for manufacturers and suppliers are significant in terms of brand image, privacy protection and liability.

To date, there is no public cyber security standard for vehicles. Therefore manufacturers and suppliers can not rely on shared references and each one has adopted a specific strategy. That leads to a lack of knowledge transfer and interoperability when attackers are becoming more organized and attack methods (and their modes) are evolving very fast.

Even the functional safety standard (ISO 26262 - 2011) dedicated to automotive, widely applied, does not address this aspect for now (whereas a working group is planning to add cyber security requirements extending this standard).

Some standards (ISO 15408, IEC 62443) or frameworks (CSPN, RGS, NIST Cyber Framework) in cyber security exist but they are generic and they do not take into account specificities of vehicles.

The present guidelines, based on automotive specificities, present best practices to address cyber security risks.

1.3. Automotive ecosystem

Cars, like most of devices we use nowadays, are becoming more connected. Those connections to data banks and tiers services involve a bigger cyber attack possibility.

Those threats enforce all actors engaged in vehicle design and maintenance to change their way of work and orientate it securely. This security management is complex because development requirements come from the manufacturer (responsible at the vehicle level and its associated functions) and are then cascaded to suppliers like tier 1 (ECU or sensor suppliers) to tier x (i.e. electronic components distributors).

Maintenance operators also have to be aware of those threats to put back all barriers specified by the manufacturers. Thus, all those actors need to exchange information and work together to improve the overall cyber security state of the automotive domain.

1.4. Methodology

These guidelines identify objectives that enable reducing cyber security risks.

They are inspired by two reputable norms widely used in their respective industry:

- ISO 26262 that defines functional safety standards to the automotive industry. The present guidelines use the ISO 26262 structure and wording to ease their integration. The guidelines keep the concept of safety integrity level.
- ISO 27001 that pertains to Information Security Management. Around a «Plan Do Check Act» cycle (based on continuous improvement), it proposes a systematic approach to deliver IT/IS products or services with the appropriate level of security, safety and confidentiality.

1.5. Guidelines structure

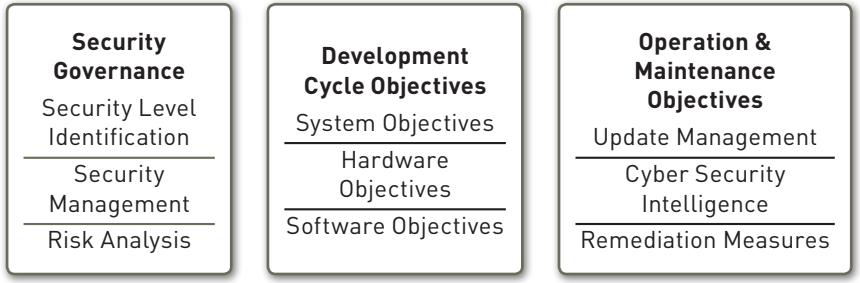


Figure 1.1: Detailed structure of the guidelines

The different objectives are distributed in 3 main parts:

- **Security Governance:** Strategy for managing the risk of cyber attacks during the lifecycle of the vehicle.
- **Development Cycle Objectives:** Specific objectives during the design phase of the vehicle.
- **Operation and Maintenance Objectives:** Specific objectives relevant to a released vehicle.

For each part of the guidelines, some objectives are defined. An objective to achieve is given as follow:

How to read the objectives

(M) (S) — Objective reference — Objective title

Description of the objective.

If (M) is present, it means that it is applicable for Manufacturer.

If (S) is present, it means that it is applicable for Supplier.

If (M) (S) is present, it means that it is applicable for both.

OBJ_GOV_XXX is an objective for Security Governance

OBJ_DEV_XXX is an objective for the Development phase

OBJ_OPE_XXX is an objective for the Operation & Maintenance phases

1.6. Definitions

- **ASSET.** Anything that has value to the organization. (ISO 27000).
- **AUTHENTICATION.** Provision of assurance that a claimed characteristic of an entity is correct (ISO 27000).
- **AVAILABILITY.** Property of being accessible and usable upon demand by an authorized entity. (ISO 27000).
- **CONFIDENTIALITY.** Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27000).
- **CONTROL.** Measure that is modifying risk. (ISO 27000).
- **CYBER SECURITY.** Protection of information systems from threats causing theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.
- **DESIGN PHASE.** Phase during which the architecture of the product/ service is established.
- **DOWNGRADED MODE.** Mode of operation in the presence of faults which have been anticipated in the design of the control system (IEC 62443) - also called degraded mode.
- **INTEGRITY.** Property of safeguarding the accuracy and completeness of assets. (ISO 27000).
- **MAINTENANCE PHASE.** The maintenance phase consists of maintenance tasks to keep the product up and running. The maintenance includes any general enhancements, changes and additions, which might be required by the end-users.
- **OPERATION PHASE.** The operation and maintenance phases occur simultaneously, the operation-phase consists of activities like assisting users in working with the created product.
- **RISK.** Effect of uncertainty on objectives (ISO 27000). Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. (ISO 27000).
- **SECURITY.** Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO 27001).
- **SECURITY LEVEL.** Measure of confidence that the system is free from vulnerabilities and functions in the intended manner. (IEC 62443).
- **SOFTWARE ITEM.** A software item is any identifiable part of a software product.

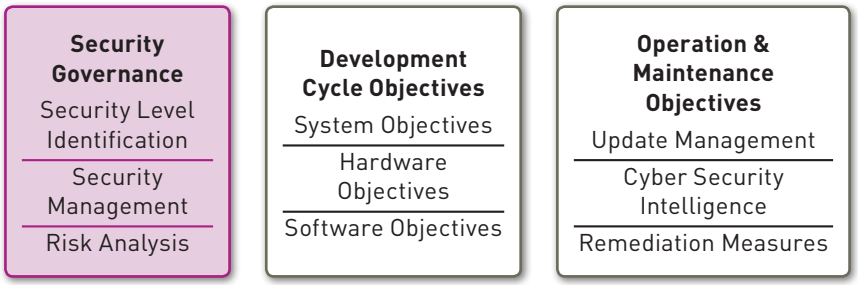
- **SOFTWARE PRODUCT.** A software product is made up of a set of computer programs. In addition to programs, the term software product may also include the associated procedures, documentation, or data. A software product may be part of another software product, may be used to develop other software products, or may be a product that has been designated for delivery to customers.
- **STACK CANARY.** A value that, when destroyed by a stack buffer overflow, shows that a buffer preceding it in memory has been overflowed. By verifying the canary value, execution of the affected program can be terminated, preventing it from misbehaving.
- **SYSTEM.** Set of interacting or interdependent component parts forming a complex/intricate whole.
- **THREAT.** Potential cause of an unwanted incident, which may result in harm to a system or organization. (ISO 27000).
- **VULNERABILITY.** Weakness of an asset or control that can be exploited by one or more threats. (ISO 27000).

1.7. Abbreviations

- **ADAS** Advanced Driver Assistance Systems
- **ADB** Android Debug Bridge
- **DEP** Data Execution Prevention
- **ECU** Electronic Control Unit
- **EVITA** E-safety Vehicle Intrusion Protected Applications
- **GCC** GNU Compiler Collection
- **HAZOP** HAZard and Operability studies
- **IDS** Intrusion Detection System
- **ISMS** Information Security Management System
- **IS** Information System
- **IT** Information Technology
- **LOPA** Layer Of Protection Analysis
- **MAC** Message Authentication Code
- **OBD** On Board Diagnostics
- **PDCA** Plan Do Check Act
- **PRNG** Pseudo-Random Number Generator
- **SL** Security Level
- **SIEM** Security Information and Event Management

OBJECTIVES

2. Security Governance



With the simultaneous increase of the attack surface and the cyber risk, it is necessary to set up a real security governance on vehicles. This goes beyond mere compliance with safety rules during the design, but involves putting up a real Information Security Management System throughout the vehicle life cycle. The sophistication of this process must be adapted to the challenges and risks.

Thus this chapter firstly describes how to assess the challenges and assets that must be protected in order to determine a level of security to attain, then gives requirements on the ISMS itself and finally explains how the risks should be evaluated.

2.1. Security Level description & assessment guidance

This section describes performance criteria to protect the vehicle from internal and external threats. It gives objectives to the manufacturer or the supplier to help them to adopt an appropriate stance towards cyber threats.

The objectives apply to a product which can be either an ECU, a set of ECUs or the complete vehicle, so they have to be checked during the whole life cycle of the product. They can be about process measures as well as supporting processes.

The main goal is to reduce the cyber risks. Each manufacturer has to define risks applicable to his business in order to take them into account. Risks can concern either the Confidentiality of the data, the Integrity of the vehicle (including the passengers, their environment and the takeover of the vehicle) or the Availability of vehicle services.

Keeping this in mind, specific and gradually-increasing efforts shall be performed to achieve the security objectives.

The analysis has to take into account the level of automation of the car (e.g. ADAS with Autopilot, driver-helping sensors) to refine risks analysis accordingly.

Those guidelines have objectives that are spread in 3 levels (Security Level, SL) to reflect the gradual implementation of the security management process.

Each Security Level includes the lesser ones in terms of objectives.

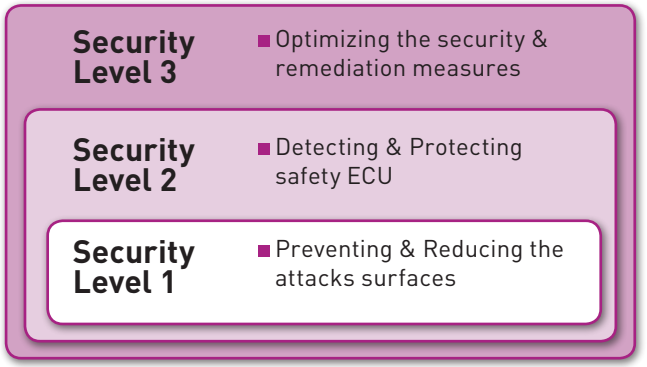


Figure 2.1: Goals and key points for each Security Level

- **Security Level 1:** this level defines the fundamental cyber security objectives that a slightly connected vehicle should reach. Easy counter measures have to be implemented at the system level to minimize risks during operational phase.
- **Security Level 2:** this level shall allow identification of cyber vulnerabilities to adopt measures to protect sensitive (safety) ECUs. Specific architecture rules have to be set to protect sub parts of the system.
- **Security Level 3:** this level allows a solid confidence in the cyber security management involving a fine analysis of all the components of the system. Analyses are done for every operating modes. In case of cyber attacks, the system is able to continue his service potentially with downgraded modes. At this level, the expectation is not only to manage the security but also to optimize it (continuous improvement process).

The targeted security level depends on several factors. It is the responsibility of the manufacturer to perform a high-level risk analysis taking into account all stakeholders requirements.

To assist in this process, the following questionnaire can be used:

- What is the level of automation driving of the car (refer to the SAE J3016 levels of automation)?
- What is the level of connectivity of the car (define scale from 1 to 5)?
- What are the legal or financial consequences of a security breach?
- What is the impact on the safety of individuals?

(M) — OBJ_GOV_10 — Security criteria

The Availability, Confidentiality and/or Integrity criteria shall be selected and defined for each relevant asset or resource that the vehicle may expose directly or indirectly to cyber attacks.

A list of assets is given as example Such assets could be: driving subsystem, upgradable firmware, driver's contacts list, navigation system history or current destination, credit card number (for self-service vehicles).

This resource list shall be representative of all the business, safety or privacy impacts that a failure of the embedded systems may have.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_20 — Security goals identification

Considering the financial, health, safety, environmental and privacy consequences of the cyber threats, a threat analysis shall be performed to identify the security goals in regard of the security criteria above.

This analysis could be done with any appropriate methodology (such as LOPA or HAZOP). Several methods such as EBIOS or MEHARI can also be used.

A specific attention shall be carried out to take into account the usage domain of the product. All identified security goals should be documented.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_30 — Security levels identification

An appropriate level (Security Level 1, 2 or 3) of protection matching the security goals that the product requires shall be selected (cf. Figure 2.1).[a]

[SL1, SL2, SL3]

[a] To help identify the appropriate level, one can refer to the ANSSI's guide «Cybersecurity for Industrial Control Systems: classification methods».

2.2. Security management

The goal of the security management process is to preserve the confidentiality, integrity and availability of relevant assets by applying a risk management process and to give stakeholders the assurance that risks are adequately managed.

(M) — OBJ_GOV_40 — Security management

A basic security management process shall be implemented. A specific person or team (called «security administrative manager» in the remainder) must be designated to take part to, document and keep records of the activities described in this guide.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_50 — Dedicated team

Cyber security activities shall be performed by a skilled and experienced team in cyber security, accustomed to cyber security matters.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_60 — Staff training

Regular trainings and workshops shall be scheduled to ensure that cyber security and safety teams maintains an up-to-date knowledge of these fields.

[SL1, SL2, SL3]

(M) — OBJ_GOV_70 — Security management integration

For a Security Level 2 and above, the security management process shall be an integral part of the overall vehicle or component program management. Cyber security must be taken into account in the design of hardware, software and maintenance components. It is expected that the security management process evolves according to the overall program needs.

[SL2, SL3]

(M) — OBJ_GOV_80 — Security management

The overall program management shall plan, implement and control processes necessary to meet the security requirements specified in this document. The program management shall also implement plans to achieve information security objectives defined in 2.1. The security manager shall retain documented information sufficient to be confident that the processes were operated as planned.

[SL2, SL3]

(M) — OBJ_GOV_90 — Security management

For a Security level 3, the security management process shall comply with all the requirements of ISO 27001 [a]. An ISO 27001 certification is strongly recommended.

The performance of the security management process must be evaluated through:

- Relevant indicators
- Internal audits
- Periodic review by the overall Program Management

[a] In particular, the security manager should implement a continuous improvement process.

[SL3]

2.3. Risk analysis

(M) (S) — OBJ_GOV_100 — Risk analysis: basic scope

This analysis has to remain global and should focus on risks relevant to operational phase.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_110 — System description

The description of the vehicle shall include all the features and their entry points & connectors (e.g hardware and the connections media).

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_120 — Risk analysis: completeness of the scope

Each entry point identified shall be mapped with identified risks in order to ensure that the attack surface is correctly mapped and identified.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_130 — Risk analysis: Action plan formal approval

The action plan shall be a formally sign off by the program manager, the security manager and the safety manager.

[SL1, SL2, SL3]

(M) (S) — OBJ_GOV_140 — Extended system description

All the electronic components of the vehicle shall be identified and characterized with their current revision/version.

All the internal buses linking the sensors, ECU and actuators shall be identified.

[SL2, SL3]

(M) (S) — OBJ_GOV_150 — Risk analysis: extended scope

For a Security level 2 and above, an extended risk analysis is mandatory to check the impact of cyber attacks on safety components. It shall include the following steps:

- Identify and describe every attack surface of the system.
- Identify and categorize every known threat.
- Perform a specific analysis for every «safety-critical» component is required (ECUs,...). This analysis shall be separated in two sub-analysis: hardware and software.
- Describe the scope of the operational and maintenance processes.
- Check that every privilege of the components have the least permissions needed.

An action plan shall be drafted.

[SL2, SL3]

(M) (S) — OBJ_GOV_160 — Share information with safety team

Results of all cyber security analyses have to be shared and discussed with the safety teams. Moreover, results from safety teams (e.g FMEA, Fault-trees) shall be taken into account for cyber security analyses.

Meetings and peer reviews shall be organized between safety & cyber-security teams.

[SL2, SL3]

(M) (S) — OBJ_GOV_170 — Exhaustive system description

The system has to be exhaustively described. Each component has to be listed, as well as every interface and functionality.

[SL3]

(M) (S) — OBJ_GOV_180 — Exhaustive risk analysis

For a Security level 3, an exhaustive risk analysis is mandatory, and shall include every component listed previously. The aim is to verify that each vulnerability has an adapted counter measure.

The analysis shall include every aspect of the car timeline (design & development, production, operation and maintenance).

[SL3]

3.Development Cycle Objectives

Security Governance	Development Cycle Objectives	Operation & Maintenance Objectives
Security Level Identification	System Objectives	Update Management
Security Management	Hardware Objectives	Cyber Security Intelligence
Risk Analysis	Software Objectives	Remediation Measures

The objectives which are described below are about the development life cycle, from the design phase to testing activities.

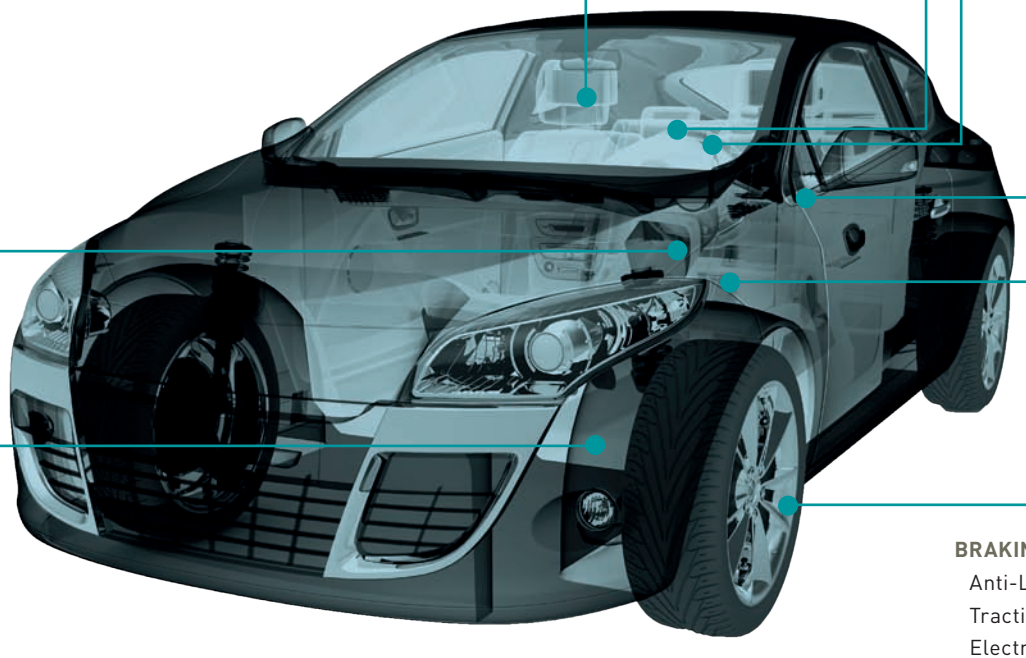
AIRBAGS
- Driver & Passenger Airbags
- Self & Passive Venting
- Low Risk Deployment
- Knee and Side Airbags
- Curtain and Rollover Airbags
- Inflator Technology

DRIVER ASSIST SYSTEMS
- Adaptive Cruise Control
- Lane Assist Systems
- Automatic Emergency Braking
- Emergency Steering Assist

SEMI-AUTOMATED DRIVING
- Traffic Jam Assist
- Highway Driving Assist

STEERING WHEEL SYSTEMS
- Touch Sensor in Steering Wheel Rim
- Hands Off Detection
- Vibrating Steering Wheel
- Illumination technology
- Contactless Horn System
- Path-free use of Horn
- Steering Wheel with Integrated Microphone
- Electrical Connections
- Heated Steering Wheel

BODY CONTROL SYSTEMS
- Integrates Electronic Control Panels (IECP)
- Steering Column Control Modules (SCCM)
- Switches and Switch Module
- HVAC (Heating, Ventilation, Air Conditioning)
- Sensors
- Access Systems



STEERING SYSTEMS
- Electrically Powered Hydraulic Steering
- Electrically Powered Steering Column Drive
- Electrically Powered Steering Rack Drive

ELECTRONICS
- Electronic Control Units
- Airbag Control Units
- Video and Radar Sensors
- Integrated Sensors
- Safety Domain ECU
- Pedestrian Protection
- Crash Sensors
- Tire Pressure Monitoring

BRAKING SYSTEMS
- Anti-Lock Braking (ABS)
- Traction Control
- Electronic Stability Control
- Slip Control Boost
- Integrated Brake Control
- Electric Park Brake
- Calipers / Rotors
- Actuation

3.1. System objectives

(M) (S) — OBJ_DEV_010 — Documentation

All the analysis have to be registered in a document compiling the cyber security requirements, performed activities and their results.

This document shall include all the reports (analysis, penetration tests results), audits, current and future security policies.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_020 — Documentation confidentiality

Each cyber security document shall remain confidential and their diffusion should be restricted on par with the sensitivity of the information carried.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_030 — Embedded systems passwords management

For every component that implements a password-based authentication (e.g. debug mode for ECUs), passwords security shall be on par with state-of-the-art recommendations[(a)].

It implies, for example, default passwords modification for Tier-1/Tier-2 integrated components, password length checking, entropy checking, password reusage prohibition,...

Hardcoding passwords is not allowed.

[(a)]For instance OWASP (https://www.owasp.org)

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_040 — Penetration tests: basic level

Penetration tests are mandatory at system level. These tests include:

1. Information Gathering

- Broadcasted Wi-Fi SSID, Bluetooth identifier, RFID networks frequencies,...
- Visual inspection of accessible information (outside and inside the car): part number, hidden ports,...

2. Vulnerability Scanning

- Wi-Fi, Bluetooth networks
- USB ports
- Common RFID hacks
- Connect compromised smartphone

3. Report on findings

- Assign a level of severity to each finding
- Assess global risk level
- Highlight remediations to reduce risk to an acceptable level

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_050 — Consolidate results

Reports produced at the checking step shall be formally reviewed by all involved parties (e.g. internal auditor, program manager, safety manager). If any gap is detected between expected behavior and tests results, it shall be documented along with the decision of what needs to be done:

- Accept the gap until next scheduled version
- Do new modifications to remove the gap immediately

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_060 — Update Risk Analysis

Residual risk should be assessed again after taking into account the actual modifications made. An action plan for residual risk shall be formally drawn and monitored.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_070 — Propagate Results

The following documents shall be made available on demand:

- Documented decision regarding any gap left
- Action plan for residual risk

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_080 — Major vulnerabilities verification

The Major Vulnerabilities listed in Annex A shall be taken into account within the risk analysis.

[SL2, SL3]

(M) (S) — OBJ_DEV_090 — Action Plan: Major vulnerabilities

A dedicated document shall be created to follow up on Major Vulnerabilities. This document shall be updated at each phase of the product life cycle. If a Major Vulnerability has no corresponding action in the action plan, it has to be justified.

[SL2, SL3]

(M) (S) — OBJ_DEV_100 — Follow up on Major Vulnerabilities

Residual risk related to Major Vulnerabilities shall be considered.

[SL2, SL3]

(M) (S) — OBJ_DEV_110 — Network equipments mapping

All the network components (e.g. firewalls, routers, gateways) shall be described with their configurations. An analysis shall be done to check their resistance to cyber attacks.

[SL2, SL3]

(S) — OBJ_DEV_120 — Passive protection & detection

Passive protections shall be used to detect cyber attack. These protections shall at least detect any malicious activity regarding messages exchanged between safety-critical ECUs.

[SL2, SL3]

(M) (S) — OBJ_DEV_130 — Penetration tests: advanced level

For a Security Level 2 and above, penetration tests shall be done at the network (communication) level.

1. Information Gathering

- Plug in mechanical tool to get a system map
- MITM type attack (with tool)
- Nmap (or any port scanner) on wireless components firmware

2. Vulnerability Scanning

- Search for know exploit on key components (SIM card, open source libraries,...)
- Focus on finding a possible path from high level software to low level software or hardware
- Focus on logical flaws

3. Report on findings

- Add new findings to list
- Estimate impact on a bigger picture

[SL2, SL3]

(M) (S) — OBJ_DEV_140 — Assess cyber attack detection efficiency

There shall be a formal review of the results of the cyber attack detection system(s) that includes:

- Compilation of the alerts raised
- Analyses of the results (e.g. false positive/negative, latency impact)
- Detailed assessment of the quality of the control

[SL2, SL3]

(M) (S) — OBJ_DEV_150 — Consolidate results

The alerts from the cyber attack detection system(s) shall be analyzed to be used as input on the Risk Assessment made in Risk Analysis (Cf. 2.3).

The aim is to make recommendations for the next version of the product.

[SL2, SL3]

(M) (S) — OBJ_DEV_160 — Improve the detection system

Any newly discovered weakness and/or idea to improve the detection system shall be documented and made available for the next version of the product.

[SL2, SL3]

(M) (S) — OBJ_DEV_170 — Propagate Results

If the detection system(s) would be more effectively implemented at a higher level (manufacturer for instance) or could be helped by higher level controls, this information should be made available to upper levels of design.

[SL2, SL3]

(M) (S) — OBJ_DEV_180 — Downgraded mode

A fallback strategy shall be defined in case of detected cyber attacks. In conformance with this strategy, downgraded modes shall be as well defined. The transitions (with their trigger conditions) between regular & downgraded modes shall be described.

[SL3]

(M) (S) — OBJ_DEV_190 — Active detection & protection

Active protection measures shall be implemented to block any ongoing attack or malicious activities.

[SL3]

(M) (S) — OBJ_DEV_200 — Penetration tests: in-depth level

Penetration tests are mandatory for each component or subsystem of the car. Each ECU shall be tested, and shall be free of any possible compromission.

1. Information Gathering

- Social engineering/compromise at the company level
- Static code analysis of complex systems
- Configuration audit
- Reverse engineer suspected ill-conceived functions (with mechanical tool)

2. Vulnerability Scanning & Exploits

- Write actual practical exploits
- Focus on implementation flaws (cryptographic flaws for instance)

3. Report on findings

- Add new findings to list
- Map of vulnerabilities and calculated impact on the whole chain

[SL3]

(M) (S) — OBJ_DEV_210 — Boundary testing

Limit cases shall be extensively tested when downgraded mode is activated.

[SL3]

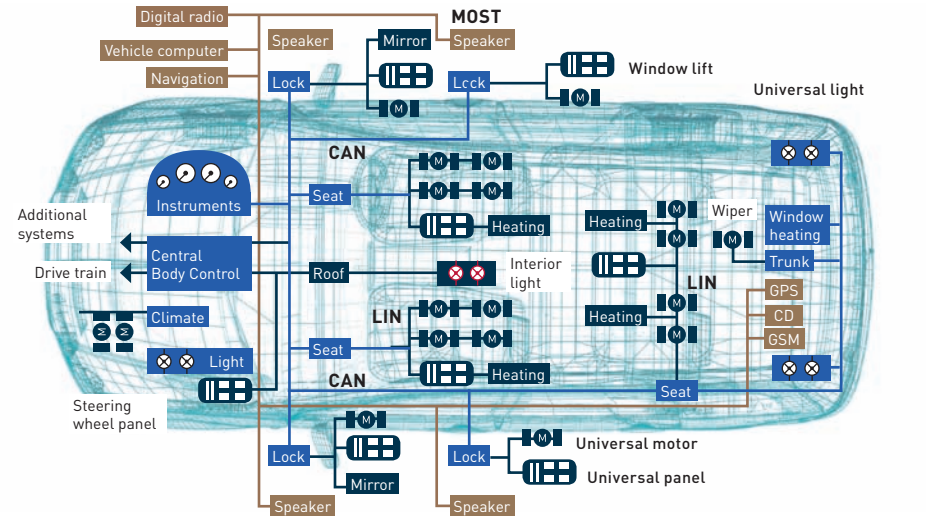


Figure 3.1: Whole system penetration tests

(M) (S) — OBJ_DEV_220 — Roll off degraded mode

Specific studies shall be done to identify conditions to move out from downgraded mode.

[SL3]

(M) (S) — OBJ_DEV_225 — Use of COTS

A cyber security certification (or at least an appropriate demonstration) is required for each COTS.

[SL3]

3.2. Hardware objectives

(M) (S) — OBJ_DEV_230 — Hardware risk analysis

During the V cycle, a basic hardware risk analysis shall be performed. This analysis can be made from a system-wide perspective.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_240 — Connectors & entry points checks

For each ECU, every physical connectors & entry points shall be documented and checked to ensure they are immune to attacks.

These entry points include physical ports (e.g USB ports, OBD connector, JTAG & UART ports on ECUs) and wireless devices (e.g Wi-Fi, Bluetooth, RFID, TPMS) entry points.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_250 — Cryptography: certified HSM for key storing

If cryptographical keys are used (e.g. for authentication and/or encryption, for filesystem encryption, for updates management), a certified secure element (HSM or equivalent) shall be used to avoid tampering or extraction.

[SL1, SL2, SL3]

(S) — OBJ_DEV_260 — In-depth hardware analysis

For each ECU and hardware component, a specific analysis is required, including a specific security risk analysis.

[SL3]

(M) — OBJ_DEV_270 — ECUs Architecture

Manufacturers shall document how ECUs are mapped to each domain of the architecture.

The mapping needs to take into account how ECUs communicate to reduce inter-domain communications[a], and thus provide an easier way to implement intrusion-detection systems (IDS).

The analysis shall also describe how the segregation is achieved (e.g. diode, gateway).

[a]The architecture can be based on the EVITA architecture, or can be generated using automated partitioning tools and techniques, such as Louvain or equivalent.

[SL3]

3.3. Software objectives

(S) — OBJ_DEV_280 — Software risks & vulnerabilities analysis

During the development cycle, a basic software risk & vulnerabilities analysis shall be performed. This analysis can be done from a system-wide perspective (attack surface approach).

Different methods (e.g. HEAVENS, OCTAVE, EBIOS, MEHARI, Attack Trees) and tools (e.g. UMLSec) can also be used to achieve this analysis.

[SL1, SL2, SL3]

(S) — OBJ_DEV_290 — Coding rules

Software development shall respect standards coding rules, such as Misra-C or ISO26262 recommendations.

[SL1, SL2, SL3]

Infotainment systems often include COTS software that dramatically increases attack surfaces, like Android system or equivalent. These systems can be run autonomously, and as such, contain a lot of options to ease software and system development.

For example, Android allows ADB debugging connections, which can be used to gain root access to the whole infotainment system.

(S) — OBJ_DEV_300 — Disabling root access & debug modes in COTS

As useful as debug connections can be in development phases, these debugging functionalities shall never be allowed in vehicles during the operational/release phases.

[SL1, SL2, SL3]

(S) — OBJ_DEV_310 — Secure boot

For every system and whenever possible, secure boot shall be used. This implies that it cannot be bypassed by another operating mode (besides normal operational mode, like debug or update mode).

[SL1, SL2, SL3]

(S) — OBJ_DEV_320 — Logs and log management

Log management policies shall be defined and implemented. This objective allows for post-mortem analysis and potentially for in-situ remediation (against an ongoing attack). Logs shall be centralized in a local (or deported) SIEM, or any equivalent system.

[SL1, SL2, SL3]

(S) — OBJ_DEV_330 — Logs protection & access

Logs are valuable assets for attackers. As such, they have to be protected against unauthorized modifications or deletion.

[SL1, SL2, SL3]

(S) — OBJ_DEV_340 — Compilation profiles

Specific compiler options can be used to increase debugging efficiency and/or security.

Release profiles shall never enable debugging flags and/or export debug symbols.

[SL1, SL2, SL3]

(S) — OBJ_DEV_350 — Safety-oriented compilation flags

Specific safety flags shall be used for compilation. These flags shall enable, at least, generation of all warnings, avoidance of code optimizations and strict programming standards compliance.

[SL1, SL2, SL3]

(S) — OBJ_DEV_360 — Cryptography: choice of protocols

Cryptographic ciphers and protocols shall be on par with state of the art recommendations. NIST Special Publication 800-175B, French Référentiel Général de Sécurité and/or NSA Suite B Cryptography can be referred to for up-to-date information.

For constrained devices, lightweight cryptography can be implemented following NIST-IR 8114, ISO 29192 and/or CRYPTREC project recommendations.

These choices shall take into account and comply with regional, national or supra-national regulatory frameworks, to maximize compliance for the purpose of certification.

[SL1, SL2, SL3]

(S) — OBJ_DEV_370 — Cryptography: message authentication

Messages from critical ECUs shall at least be authenticated using MAC.

[SL1, SL2, SL3]

(S) — OBJ_DEV_380 — Cryptography: X.509 mutual authentication of external devices

External devices used for diagnostics, updates, or any kind of operations involving modifications of software or parameters shall be mutually authenticated using valid X.509 certificates before performing operations.

[SL1, SL2, SL3]

(M) (S) — OBJ_DEV_390 — Protocols description

Each communication and cryptographic protocol shall be described and shall be matched to each component using it. Also, each cryptographic choice made (e.g. key length, PRNG choice) shall be justified and documented.

Each communication and cryptographic protocol shall be described and shall be matched to each component using it. Also, each cryptographic choice made (e.g. key length, PRNG choice) shall be justified and documented.

[SL2, SL3]

(S) — OBJ_DEV_400 — Toolchain hardening: ASLR – Address Space Layout Randomization

Randomly arranges the address space positions and help prevents buffer overflows[(a)].This functionality is also known as Position Independent Executable (PIE). If available, this functionality (or equivalent) should be used.

[(a)]Note that the efficiency of ASLR highly depends on the available address search space, and is reduced for 32-bits systems.

[SL2, SL3]

(S) — OBJ_DEV_410 — Toolchain hardening: Stack Smashing Protection

Another way of guarding against buffer overflow exploitation is to use a stack-smashing protection. This technique add a «stack canary» for a set of critical functions which will be verified when calling the return instruction. By verifying the value of the canary at the end of the function, the program can be automatically terminated in case of an incorrect value of the canary.

While this technique is very effective at preventing buffer overflows, the automatic termination of the program can be detrimental in terms of safety or availability, and thus its activation shall be extensively tested.

[SL2, SL3]

(S) — OBJ_DEV_420 — Toolchain hardening: NX bit

The NX bit, also known as DEP, is a hardware-based executable-space protection.

It is used to segregate areas of memory, and marks them as nonexecutable, thus preventing malicious or external code from being executed when injected in these areas.

If available, this functionality (or equivalent) should be used.

[SL2, SL3]

(S) — OBJ_DEV_430 — Toolchain hardening: Source fortifying

Fortifying sources helps prevent buffer overflows by checking deprecated and dangerous functions, such as memcpy, mempcpy, memmove, memset, stpcpy, strcpy, strncpy, strcat, strncat, sprintf, snprintf, vsprintf, vsnprintf, and gets. C programs can be extended with StrSafe.h and banned.h files from Microsoft SDL.

If available, this functionality (or equivalent) should be used.

[SL2, SL3]

(S) — OBJ_DEV_440 — Toolchain hardening: compiler selection and maintenance

Use of a industry-grade and up-to-date compiler is strongly recommended. If a legacy version shall be used with no possibility of upgrading, a vulnerability and critical bugs check & follow-up shall be performed.

[SL2, SL3]

(S) — OBJ_DEV_450 — Toolchain hardening (LLVM/Clang): sanitizers

Recent GCC and LLVM releases include new debugging tools, called sanitizers, that help find tricky bugs, undefined behaviors, memory problems and buffer overflows. They shall be used when deemed possible (at least in debug releases when the performance impact is too important for a release build[(a)]).

A partial list is presented below:

- AddressSanitizer: detects memory bugs
- ThreadSanitizer: detects data races
- LeakSanitizer: detects memory leaks at run-time
- MemorySanitizer: detects uninitialized reads
- UndefinedBehaviorSanitizer: detects undefined behavior

[(a)]You can benchmark the overhead with SanitizerStats: http://clang.llvm.org/ docs/SanitizerStats.html

[SL2, SL3]

(M) (S) — OBJ_DEV_460 — Cryptography: Message authentication

Robust HMACs-based communications with keys and hash algorithms on par with state of the art recommendations[(a)] shall be used to authenticate messages.

[(a)]e.g. French Référentiel Général de Sécurité or «ECRYPT II Yearly Report on Algorithms and Keysizes» from Ecrypt II

[SL2, SL3]

(S) — OBJ_DEV_470 — Rights & permissions management

Software shall always run with the lowest privileges possible.

[SL2, SL3]

(S) — OBJ_DEV_480 — Software static analysis

Critical software shall be analyzed using a sound static analysis tool.

[SL3]

(S) — OBJ_DEV_490 — Formally verified compiler

Usage of a formally verified compiler, such as CompCert for C programs, shall be considered.

[SL3]

(S) — OBJ_DEV_500 — Software safety integrity level

The software shall have a level of maturity based on safety standards (e.g. ASIL C for ISO 26262, SIL 3 for IEC 61508, SC 3 for BV-SW-100).

[SL3]

OBJECTIVES

4. Operation & Maintenance Objectives

These objectives are about the operational and maintenance phases of the lifecycle.

(M) (S) — OBJ_OPE_010 — Patches integrity

Patches shall always be authenticated and signed before release & deployment. Their installation shall verify these two properties before performing the update process.

[SL1, SL2, SL3]

(M) (S) — OBJ_OPE_020 — Patches deployment

Patches shall be securely dispatched to final customers. This can be done directly through an Over-The-Air update process, or through garages during periodical checks.

In either cases, a secure deployment policy shall be implemented and maintained.

[SL1, SL2, SL3]

(M) (S) — OBJ_OPE_030 — Factory reset

A procedure shall be defined to erase and sanitize user data present in the system.

[SL1, SL2, SL3]

(M) (S) — OBJ_OPE_040 — End of life

A procedure shall be defined to erase and sanitize sensitive data present in the system before the disposal of the system.

[SL1, SL2, SL3]

(M) (S) — OBJ_OPE_050 — Active protection system updates

When an active protection solution is implemented, an update procedure and process shall be set up. This process shall only be performed through a secure deployment channel.

[SL1, SL2, SL3]

(M) (S) — OBJ_OPE_060 — Cyber security Intelligence

Because cyber security threats constantly evolve, a continuous survey shall be performed to ensure that the system is still immune to latest threats or vulnerabilities discovered.

[SL2, SL3]

(M) — OBJ_OPE_070 — Garages & repair shops security policy

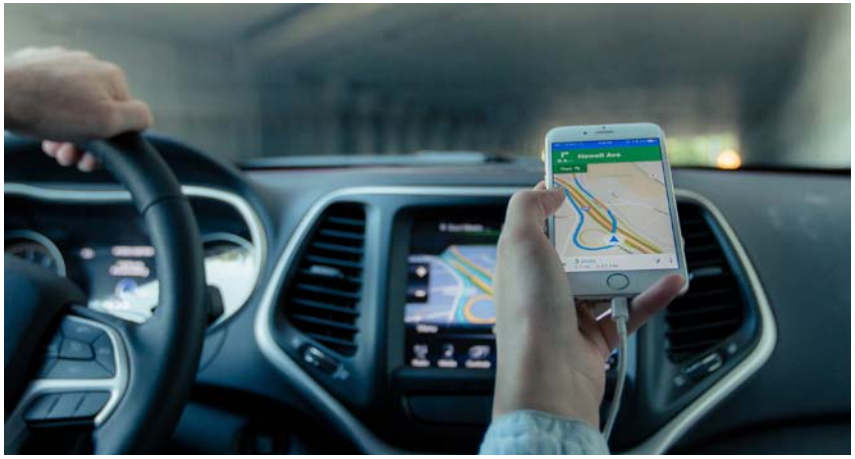
For affiliated garages, a security policy shall be implemented to ensure that their networks and tools are not compromised or used by a malicious attacker.

[SL2, SL3]

(M) (S) — OBJ_OPE_080 — Recovery plan

A recovery plan shall be written and maintained.

[SL3]



ANNEXES +

Annex A: Major vulnerabilities & risks

Those are the major vulnerabilities & risks identified, thus they are required to be checked for:

- Memory buffers problems (e.g. out-of-bounds, overflows)
- Access control & credentials
- Information exposure
- Improper input validation
- Possibility of code injection
- Cryptographic misuse or absence
- Usage of unsafe/dangerous or deprecated functions (strcpy...)
- Bad and/or non-standard implementations (Bluetooth, cryptography, custom libraries...)
- No usage of binary hardening options (e.g. ASLR, DEP)
- No dedicated cyber security process
- No dedicated cyber security team

Annex B: Objectives matrix

OBJECTIVE	SL 1	SL 2	SL 3	MANUFACTURER	SUPPLIER	P/D/C/A
2. SECURITY GOVERNANCE						
2.1. Security Level description & assessment guidance						
OBJ_GOV_010	X	X	X	X		P
OBJ_GOV_020	X	X	X	X	X	P
OBJ_GOV_030	X	X	X	X	X	P
2.2. Security Management						
OBJ_GOV_040	X	X	X	X		P
OBJ_GOV_050	X	X	X	X	X	P
OBJ_GOV_060	X	X	X	X	X	D
OBJ_GOV_070		X	X	X		P
OBJ_GOV_080		X	X	X		P
OBJ_GOV_090			X	X		P
2.2. Risk Analysis						
OBJ_GOV_100	X	X	X	X	X	P
OBJ_GOV_110	X	X	X	X	X	P
OBJ_GOV_120	X	X	X	X	X	P
OBJ_GOV_130	X	X	X	X	X	D
OBJ_GOV_140		X	X	X	X	P
OBJ_GOV_150		X	X	X	X	P
OBJ_GOV_160		X	X	X	X	D
OBJ_GOV_170			X	X	X	D
OBJ_GOV_180			X	X	X	P

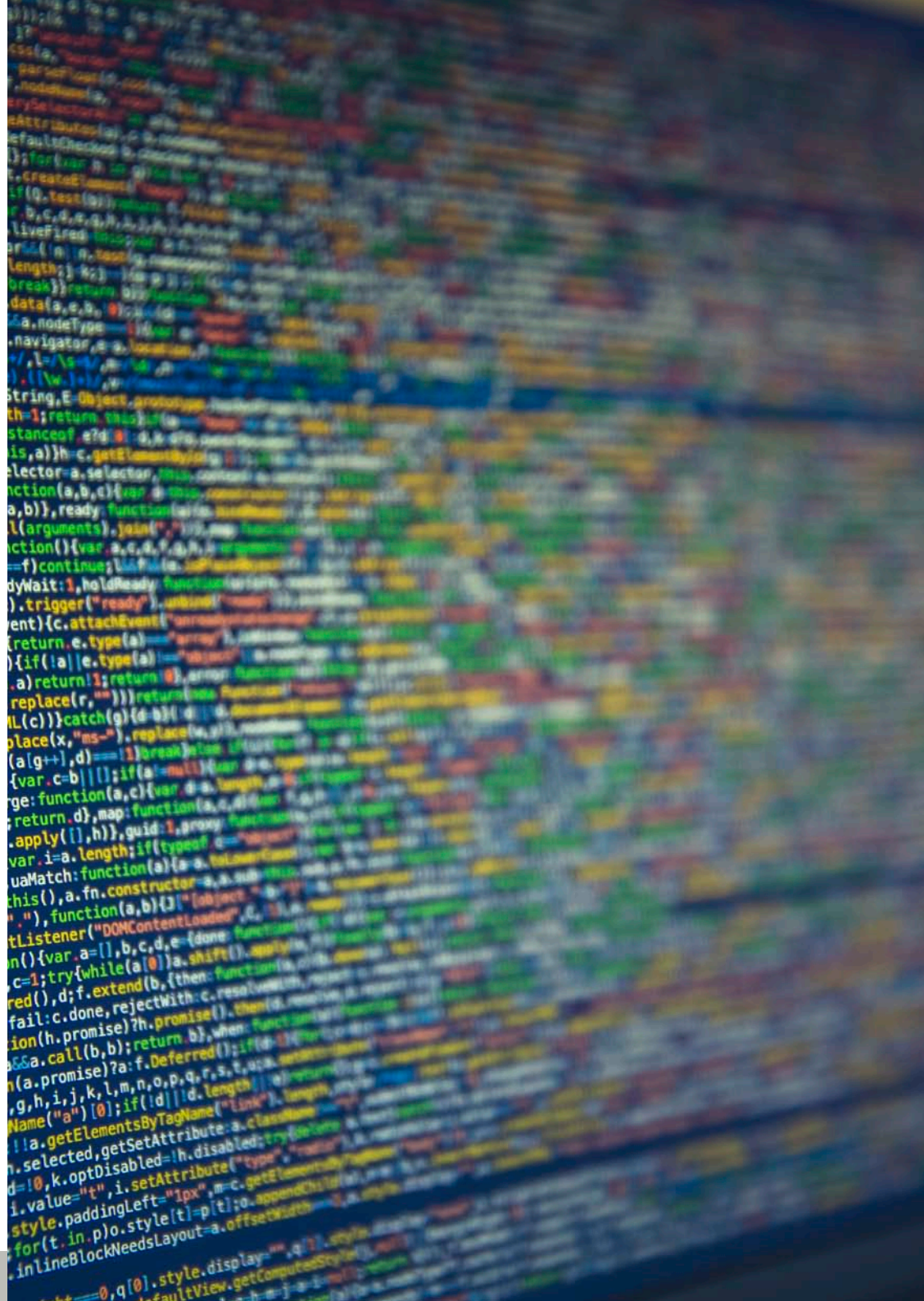
OBJECTIVE	SL 1	SL 2	SL 3	MANUFACTURER	SUPPLIER	P/D/C/A
3. DEVELOPMENT CYCLE OBJECTIVES						
3.1. System objectives						
OBJ_DEV_010	X	X	X	X	X	D
OBJ_DEV_020	X	X	X	X	X	D
OBJ_DEV_030	X	X	X	X	X	D
OBJ_DEV_040	X	X	X	X	X	C
OBJ_DEV_050	X	X	X	X	X	A
OBJ_DEV_060	X	X	X	X	X	A
OBJ_DEV_070	X	X	X	X	X	A
OBJ_DEV_080		X	X	X	X	P
OBJ_DEV_090		X	X	X	X	P
OBJ_DEV_100		X	X	X	X	D
OBJ_DEV_110		X	X	X	X	D
OBJ_DEV_120		X	X		X	D
OBJ_DEV_130		X	X	X	X	C
OBJ_DEV_140		X	X	X	X	C
OBJ_DEV_150		X	X	X	X	A
OBJ_DEV_160		X	X	X	X	A
OBJ_DEV_170		X	X	X	X	A
OBJ_DEV_180			X	X	X	P
OBJ_DEV_190			X	X	X	D
OBJ_DEV_200			X	X	X	C
OBJ_DEV_210			X	X	X	C
OBJ_DEV_220			X	X	X	A
OBJ_DEV_225			X	X	X	D
3.2. Hardware objectives						
OBJ_DEV_230	X	X	X	X	X	P
OBJ_DEV_240	X	X	X	X	X	C
OBJ_DEV_250	X	X	X	X	X	D
OBJ_DEV_260			X		X	P
OBJ_DEV_270			X	X		D

OBJECTIVE	SL 1	SL 2	SL 3	MANUFACTURER	SUPPLIER	P/D/C/A
3.3. Software objectives						
OBJ_DEV_280	X	X	X		X	P
OBJ_DEV_290	X	X	X		X	D
OBJ_DEV_300	X	X	X		X	D
OBJ_DEV_310	X	X	X		X	D
OBJ_DEV_320	X	X	X		X	D
OBJ_DEV_330	X	X	X		X	D
OBJ_DEV_340	X	X	X		X	D
OBJ_DEV_350	X	X	X		X	D
OBJ_DEV_360	X	X	X		X	D
OBJ_DEV_370	X	X	X		X	D
OBJ_DEV_380	X	X	X		X	D
OBJ_DEV_390		X	X	X	X	D
OBJ_DEV_400		X	X		X	D
OBJ_DEV_410		X	X		X	D
OBJ_DEV_420		X	X		X	D
OBJ_DEV_430		X	X		X	D
OBJ_DEV_440		X	X		X	D
OBJ_DEV_450		X	X		X	D
OBJ_DEV_460		X	X	X	X	D
OBJ_DEV_470		X	X		X	D
OBJ_DEV_480			X		X	C
OBJ_DEV_490			X		X	D
OBJ_DEV_500			X		X	D

OBJECTIVE	SL 1	SL 2	SL 3	MANUFACTURER	SUPPLIER	P/D/C/A
4. OPERATION & MAINTENANCE OBJECTIVES						
OBJ_OPE_010	X	X	X	X	X	D
OBJ_OPE_020	X	X	X	X	X	D
OBJ_OPE_030	X	X	X	X	X	D
OBJ_OPE_040	X	X	X	X	X	D
OBJ_OPE_050	X	X	X	X	X	D
OBJ_OPE_060		X	X	X	X	D
OBJ_OPE_070		X	X	X		D
OBJ_OPE_080			X	X	X	P

Annex C: Bibliography

- ISO 26262 (2011): Road vehicles - Functional safety
- ISO ISO 29192 (2012 - 2016): Lightweight cryptography
- IEC 27001 (2013): Information technology – Security techniques
- RGS (V2.0): Référentiel Général de Sécurité (ANSSI)
- IEC 62443-2-1 (2010): Establishing an industrial automation and control system security program
- IEC 62443-3-3 (2013): System security requirements and security levels
- ISO 15408 (2009) / Common Criteria: Information technology – Security techniques – Evaluation criteria for IT security
- SAE J3016 (2014): Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems
- CSPN (ANSSI): Certification de Sécurité de Premier Niveau
- Cybersécurité des systèmes industriels : mesures détaillées (ANSSI)
- EBIOS method (2010): http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
- MEHARI method (2010): https://clusif.fr/mehari/
- NIST Cyber framework : https://www.nist.gov/cyberframework
- OCTAVE method (1999): http://www.cert.org/octave
- ICT-2007-216676 (ECRYPT II - 2011-2012): ECRYPT II Yearly Report on Algorithms and Keysizes
- EVITA (2012): E-safety Vehicle Intrusion Protected Applications - http://www.evitaproject.org/
- CRYPTREC: Cryptography Research and Evaluation Committees - http://www.cryptrec.go.jp/english/index.html
- NISTIR 8114 (2016): Report on Lightweight Cryptography
- OWASP Project: https://www.owasp.org
- N. Nowdehi, P. Kleberger and T. Olovsson, «Improving in-vehicle network architectures using automated partitioning algorithms,» Vehicular Networking Conference (VNC), 2015 IEEE, Kyoto, 2015, pp. 259-266. doi: 10.1109/VNC.2015.7385585
- CommonWeakness Enumeration (CWE): https://cwe.mitre.org/
- Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/



Move Forward with Confidence

Bureau Veritas SA
Société Anonyme – RCS registration number: B 775 690 621 R.C.S Nanterre
Head office address: 67/71, boulevard du Château – 92200 Neuilly-sur-Seine
contactramsmail@fr.bureauveritas.com
www.bureauveritas.com